The Chalfonts Community College

E- Safety Policy

2022-2023

Approved by:	RFL Committee	Date: 22nd November 2022
Last reviewed on:	November 2022	
Next review due by:	November 2023	

Contents

1. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scam

2. Legislation and guidance

This policy is based on the Department for Education's (DfE) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for Principals and school staff
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL).

All governors will:

- Ensure that they have read and understand this policy
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with SEND because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's DSL (and Deputies) are set out in our Child Protection Policy as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Principal, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school Child Protection policy
- Ensuring that online safety incidents are logged on CPOMS and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety where relevant
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Principal and/or governing board

This list is not intended to be exhaustive.

3.4 The ICT manager

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems, which are reviewed and updated on a regular basis to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy (this is completed in conjunction with the DSL Team)

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

- Notify a member of staff or the Principal of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International
- Healthy relationships – Disrespect NoBody campaign - GOV.UK (www.gov.uk)

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2)

4. Educating pupils about online safety

Pupils will be taught about online safety as part of the curriculum:

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships and sex education and health education in secondary schools

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

By the **end of secondary school**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners

- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects (like PSHCE) where relevant.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Principal.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power. (See also the School's Behaviour for Learning & Child Protection Policies)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Assemblies linked to cyber-bullying will be conducted throughout the year as and when they are required but it will also be discussed in detail annually as part of the Anti-Bullying Week in November each year.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of annual safeguarding training (see section 11 for more detail).

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Potential incidents or concerns can be reported through the anonymous reporting tool Whisper

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the school rules
- If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:
- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
- Report it to the police*
- Staff may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse includes an online element.
- Any searching of pupils will be carried out in line with:
- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All pupils, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 & 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

The Chalfonts Community College has an additional layer of ICT safeguarding through 'Smoothwall' where internet access is rigorously monitored and any concerns raised will trigger a level 1-5 alert to the DSL Team to investigate.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but they are not permitted to use them during the school day on school site in accordance with the school's Behaviour for Learning Policy and the students' Non-Negotiables displayed in every classroom.

Any breach of the acceptable use agreement by a pupil may trigger disciplinary action in line with the school's Behaviour for Leaning Policy which may result in the confiscation of their device.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Ensuring their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date – always install the latest updates

Staff members must not use the device in any way which would violate the school's terms of acceptable use, as set out in appendix 2.

Work devices must be used solely for work activities.

If staff have any concerns over the security of their device, they must seek advice from the school's IT Support Team and/or ICT Manager (Mr Richard Smith)

10. How the school will respond to issues of misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our Behaviour for Learning, ICT and Child Protection Policies. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary/Code of Conduct Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
  - Abusive, harassing, and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- develop better awareness to assist in spotting the signs and symptoms of online abuse
- develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh the risks up
- develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and Deputy DSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years in line with the Buckinghamshire Safeguarding Board. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their annual safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection Policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety on CPOMs. These concerns are dealt with in line with the school's Behaviour for Learning Policy.

This policy will be reviewed every year by the Director of Finance and Operations. At every review, the policy will be shared with the governing board.

13. Links with other policies

This online safety policy is linked to our:

- Child Protection policy
- Behaviour for Learning policy
- Staff Disciplinary procedures /Code of Conduct
- Data Protection policy
- Complaints procedure
- ICT and internet acceptable use policy

THE CHALFONTS COMMUNITY COLLEGE

APPENDIX ONE: Student Use of ICT Systems and Internet

STUDENT AGREEMENT

Network Access and Passwords

- I will take care of all ICT equipment that I use.
- I will never give my password to anyone, even my best friend. If I think someone has obtained my password, I will report this to my teacher immediately and change it.
- I will not attempt to gain unauthorised access to the Chalfonts Community College network or to any other computer system found on the Internet. I will not attempt to logon using another person's username and password, or to access another person's files.
- I will only use the network for College work and homework. My teacher, or network manager, may check the content of my files.

1. Internet and Websites

- I understand that my teacher and the Internet service provider will monitor the sites I have visited and may check the content of any email, or other message that I have sent.
- I will not use the Internet to view inappropriate material (such as racist or pornographic sites). If I am unsure if a site is suitable, I will ask a member of staff before attempting to access the site.
- I understand that information on the Internet may not always be reliable and sources may need checking.
- I will not take information from the Internet and pass it off as my own work.

2. Email and other forms of electronic communication

- I will always use email in a responsible and appropriate manner.
- I will only send and respond to emails from people I know, or that a teacher has approved.
- I will not send or respond to nasty, suggestive or rude emails or messages via bulletin boards.
- I will always be myself and will not pretend to be anyone or anything I am not.
- I will never send anyone my picture, or that of another person without permission from my teacher/parent/guardian/carer.
- I am not allowed to send large volume emails (spamming).
- I will never tell anyone I communicate with on the Internet my home address, my telephone number, my College's name, or arrange to meet anyone I communicate with on the Internet in person.
- I am not allowed to use an Internet chat room.
- I will inform the teacher of any misuse of the Internet, or email that comes to my attention.

I have read this policy and agree to follow it. I understand that disciplinary action may be taken and my Internet access may be removed if I misuse email, or the Internet and my parents/guardian will be informed.

Student's Name ……..

Signed Student ……..

APPENDIX TWO: Staff Use of ICT Systems, Internet Policy and Code of Practice Agreement

1. Important ICT Policy - To keep you safe

You are expected to follow the schools policy when using any equipment or accessing the Internet.

Network Access and Passwords

- Keep your password secure - do not share.
- It is your responsibility to prevent your User ID and Password being used by others to gain
- access to IT equipment at the College.
- It is a breach to attempt to access unauthorised areas including attempting to login to person's area.
- Computer screens **must** be locked to prevent unauthorised access when unattended.

Internet Safe Practice

- It is an offence to attempt to use equipment to access unsuitable websites of an inappropriate nature including adult material, racist or indecent sites.
- Be aware that we will routinely monitor sites and material viewed on school property.
- Adhere to copyright laws and no plagiarism.

Email

- Use email responsibly and ensure all messages are polite, respectful and appropriate about individuals/ the college.
- Sending images of students or staff is prohibited without written permission.
- Personal external email accounts should never be used in conversations between staff/students and parents.
- Staff must report any inappropriate email correspondence from or with a student to
    - Principal - inappropriate emails from staff or parents report directly to Principal.
- Staff can only engage in VLE forums. Other networking and chat site facilities with students is prohibited.
- The Vice Principal and network manager may access staff email if they believe inappropriate use.

General

- Staff may only keep information about students which is in line with the data protection legislation. Any shared information to outside parties must be sanctioned by a member of SLT.
- Content of staff files may be checked by the network manager at any time, with the permission of the Principal, if there are concerns.
- Staff must follow the procedure regarding ICT systems in the staff handbook.
- The college will cooperate with any appropriate officials, or police, in any investigation related to potentially illegal activities conducted in the college.

Loan of equipment

- Written permission from parents is required for loan of IT equipment to students outside of school.

- School equipment, if taken off site should only be used for work related activity.

2. Staff enforcement and monitoring of the Student ICT Policy

Staff must enforce and monitor ICT Policy at all times, in particular:

- If students deliberately or accidently access unsuitable materials staff should make note of student, pc and material accessed.

- Staff should monitor and scrutinize what students are accessing.

- Staff should provide clear guideline for content of email messages, sending and receiving procedures.

- Staff should provide students with skills and techniques to enable efficient and effective use of the Internet and seek opportunities to educate about safe practices.

    - Staff should ensure students have clearly defined learning focus for using the Internet and email.

- Staff should ensure that students only access the College network using approved College ICT equipment and do not allow students access to the PC/laptops allocated for teacher use.

- If you fail in your duty of care to protect yourself and the school by allowing students to access staff computers, or work areas, this will be considered to be gross misconduct and will be subject to the College's disciplinary procedures. Failure to adhere to this may result in summary dismissal.

Member of Staff's name …….

Member of Staffs signature …….

History

Date	Issue	Status	Comments
October 2022	1	New	